

U.S.S.N. 09/997,402

REMARKS – General**Claim Rejections under 35 USC §101:**

The Office Action (OA) rejects claims 30-44 as being unpatentable under 35 USC §101. Specifically, the OA notes that the claims, as originally filed, are not limited to tangible media, but instead include intangible media, for example a “transmission medium”.

Applicants have amended claims 30-44 to recite a network transmission system, comprising specific components with associated functionality. For example, claim 30 now recites a transmission system comprising a deployment manager and an inspector. These system components are shown in FIG. 7 as originally filed. Additionally, support for the amendment is found in the specification at page 27, line 3, through page 28, line 14. Applicants respectfully submit that this amended claim, and its associated dependent claims, are directed and limited to tangible elements, and thus constitute statutory subject matter under §101. Applicants respectfully request reconsideration of the rejection in light of the amendment.

Claim Rejections under 35 USC §102:

The OA rejects claims 1-10, 12, 14-20, 22-23, 24-26 and 29 under 35 USC §102(e) as being anticipated by Weinman, Jr., US Pat. No. 6,658,455, hereinafter “Weinman”. Specifically the OA submits that Weinman teaches the limitations of these claims, including provisioning content for a target device, verifying that the device supports the execution of the content requirements, and providing verified and provisioned content. Applicants respectfully traverse the rejection.

To begin, Applicants have amended claim 1 to recite a system for deploying content to a target device, where the content may be received from trusted sources, be they local or remote, or untrusted sources. Where the content comes from an untrusted source, the system intercepts and inspects the content to ensure that the content does not contain malicious code, banned code or designated API. Support for this amendment is

U.S.S.N. 09/997,402

found in the specification on page 3, lines 9-17, page 27, lines 3-22, FIG. 15, and claim 5 as originally filed.

Applicants respectfully submit that Weinman fails to teach such a system. While the OA suggests (in the rejections of claim 5) that Weinman discloses determining whether the content contains malicious code at col. 15, lines 45-67 and col. 16, lines 1-41, Applicants respectfully submit that this is not the case. In those passages, and throughout the application, Weinman discusses only a user defined "rule-base" that allows the user to determine whether to store into memory numbers and addresses (i.e. a yes/no instruction which does not include any analysis of the downloaded information prior to making the decision). (Col. 9, line 65, through col. 10, line 19.) Examples of user-defined rules provided by Weinman are whether to store or discard an operator assisted, retrieved telephone number (col. 10, lines 10-14) where information is stored (col. 10, lines 15-19); whether downloading is done automatically (col. 12, lines 7-11), whether to notify the user when new information is downloaded (col. 12, lines 12-16) whether to look for updates, like a new area code (col. 12, lines 24-32), and whether to allow games to be played on the device (col. 12, line 19).

Applicants respectfully submit that such a user-defined system is not a system that checks for malicious or banned code, or whether the code contains a designated API. Applicants respectfully submit that a user who has the options of selecting, for example, "1" for store and "0" for discard, as suggested by Weinman, is not capable of scanning to-be-downloaded code for malicious content or banned content. The only option the user has is to download the content and run it on the target device. If the device crashes, or worse is damaged or destroyed, with the invention of Weinman, the user must remember this experience and make sure to hit "0" if the information ever comes about again.

In Applicants' invention, by contrast, when content or applications are downloaded from an untrusted source, the application is checked for banned or malicious code *prior* to download and execution on a target device. This scanning looks not only for inherently malicious elements, but those that may simply be incompatible with the user's system as a whole. Additionally, as recited in amended claim 5, even locally stored content or applications may be intercepted and scanned to ensure that no malicious or banned code is included.

U.S.S.N. 09/997,402

This interception and inspection of application code ensures that the untrusted applications will run in accordance with the user's expectations when downloaded to the portable device. It also ensures that the untrusted applications will do no damage to the remote device during either download or operation. This scanning is effective because the scanning ensures the code is capable of not only running, but running effectively on the user's device.

By way of example, consider the instance where a handset ships with a particular type of software. If an untrusted, third party, requested application to be downloaded has code that, for example, causes a memory stack overflow in this handset software, with such an overflow destabilizing the handset software, the application would constitute malicious code. As the handset software may be unprepared to handle such a memory allocation, unexpected consequences may result.

If the application were downloaded and run on that device, without first scanning for the malicious components, the application may do damage to the device, the user, the subscriber network or all of the above. For instance, if the malicious code caused a memory stack to overrun, such an overrun could compromise the operability of the device. There is nothing in the user driven rule base of Weinman to stop such an occurrence from happening. In Applicant's invention, by contrast, the interception and detection of malicious or banned code prevents such harm from occurring.

As Weinman fails to teach any such screening or interception, as recited in Applicants' amended claim 1, Applicants respectfully submit that the rejection is overcome. Applicants respectfully request reconsideration of the rejection in light of the amendment. As claims 2-10, 12, 14-20, 22-23, 24-26 and 29 all depend from claim 1, Applicants respectfully submit that the rejections to these claims are also overcome.

Additionally, Applicants have amended claims 5, 7-8, and claims 11-17. Support for the amendment to claim 5 is found in FIG. 24 and in the specification at page 55, line 12, to page 56, line 8. With respect to claim 5, Applicants respectfully submit that Weinman failed to teach the deconstruction of a structure and a checking of activated threads.

The support for the amendment to claims 7-8 is found at page 27, line 23 through page 28, line 14, page 55, line 12 through page 56, line 8, and claims 4 and 7 as originally

U.S.S.N. 09/997,402

filed. Support for the amendment for claims 11-17 is found at page 51, line 3, through page 52, line 3, and in FIG. 25.

Claim Rejections Under 35 USC §103:

Claim 11 is rejected under 35 USC §103 as being unpatentable over Weinman in view of Galensky et al., US Pat. No. 6,845,398, hereinafter "Galensky". Specifically, the OA submits that Weinman teaches the limitations of claim 1, but fails to teach an optimization of code including reducing the variable size, modifying instructions to more efficient code, and removing unused code. The OA submits that Galensky teaches such a solution, and that it would thus be obvious to one of ordinary skill in the art at the time of Applicants' invention to combine Galensky and Weinman to achieve Applicants' invention. Applicants respectfully traverse this rejection.

As discussed above, Applicants respectfully submit that Weinman fails to teach a system for deploying content to a target device, where the content may be received from trusted sources, be they local or remote, or untrusted sources, further where when the content comes from an untrusted source, the system intercepts and inspects the content to ensure that the content does not contain malicious code, banned code. Applicants respectfully submit that Galensky also fails to teach such a system. As such, the combination of references fails teach all of Applicants' claimed limitations as recited in amended claim 11, as is required by MPEP §2143.03. Applicants thus respectfully submit that the rejection is overcome.

Further, Applicants respectfully traverse the assertion of the OA that Galensky teaches an optimization of code including reducing the variable size, modifying instructions to more efficient code, and removing unused code. At the sections of Galensky cited by the OA, Galensky teaches only the erasure of applications no longer in use and "reformat[ing] for transmission over a wireless network in a conventional matter." Applicants respectfully submit that this is none of reducing the variable size, modifying instructions within an application or removing unused code from an application. Applicants note that to create a prima facie case of obviousness, the combination must teach all of Applicants' claimed limitations. (MPEP §2143.03.) As the

U.S.S.N. 09/997,402

combination of Weisman and Galensky fails to do so, Applicants respectfully request reconsideration of the rejection.

Claims 13, 21 and 27-28 are rejected under §103 as being unpatentable over Weinman in view of Moles et al., Pub. No. 2003/0162533, hereinafter "Moles". Specifically, the OA submits that Weinman teaches the limitations of claim 1, but fails to teach a byte-code level of content examination. The OA submits that Moles teaches such a solution, and that it would thus be obvious to one of ordinary skill in the art at the time of Applicants' invention to combine Moles and Weinman to achieve Applicants' invention.

In response, Applicants note that the "byte-code" inspection of claim 13 has been deleted by amendment. As such, Applicants respectfully submit that the rejection is overcome. Applicants respectfully request reconsideration of the rejection.

With respect to claim 21, the OA submits that Moles teaches a Java-based content. With respect to claims 27-28, the OA submits that Moles teaches provisioning through website administration.

As note above, Applicants respectfully submit that Weinman fails to teach Applicants' invention as recited in claim 1. Further, Applicants respectfully submit that Moles fails to teach a system for deploying content to a target device, where the content may be received from trusted sources, be they local or remote, or untrusted sources, further where when the content comes from an untrusted source, the system intercepts and inspects the content to ensure that the content does not contain malicious code, banned code. Moles merely teaches the addition of a security code to an application to ensure that the data is not corrupted during transmission. Applicants respectfully submit that such a security code is not an interception and scanning for malicious code. As neither Weinman nor Moles teaches Applicants' invention as recited in the amended claims, Applicants respectfully submit that the rejection is overcome. Applicants respectfully request reconsideration of the rejections.

Further, claim 28 has been amended to recite the preparation of an initial list of available applications. Support for the amendment is found on page 16, lines 12-14.

U.S.S.N. 09/997,402

Applicants respectfully submit that Weinman and Moles fail to teach the preparation of such a list.

The OA notes that claims 30-44 are rejected upon the same grounds as claims 1-29, and are thus rejected for the same rationales. Applicants respond with the following comments:

Regarding claim 30, it has been amended to recite the ability of downloading applications from both trusted and untrusted sources, and upon downloading from an untrusted source, checking the program with an inspector. Support for the amendment is found on page 27, line 3, through page 28, line 14, and FIG. 7. Applicants respectfully submit, as noted with respect to claim 1 above, that Weinman fails to teach such a system. Further, Weinman fails to teach an inspector having the functions recited in amended claim 30. Applicants respectfully request reconsideration of the rejection in light of these comments.

Regarding claim 32, it has been amended to include the physical systems of an optimizer and instrumentation analyzer, which perform the functions of reducing code size and altering application code for more efficient downloading. Support for this amendment is found in the specification at page 26, line 20, through page 27, line 2, in combination with page 27, line 23, through page 28, line 14. Applicants respectfully submit that Weinman fails to teach such a system. Applicants respectfully request reconsideration of the rejection.

Regarding claim 33, it has been amended to recite the types of standards that the instrumentation analyzer may use to check conformity of the requested application. Support for this amendment is found on page 27, line 23, through page 28, line 14. Regarding claim 35, it has been amended to conform with newly amended claim 30, with support coming from claim 34 as originally filed. Regarding claim 36, it has been amended to recite the insertion of code by the instrumentation analyzer to implement various policies. Support for this amendment is found on page 28, line 25, through page 29, line 12. Regarding claims 39 and 40, they have been amended to recite a provisioning manager configured to verify whether a device supports the application by verifying the device. Such a provisioning manager, with the capabilities recited in the amended claim

U.S.S.N. 09/997,402

and the claims from which it depends, is not taught by Weinman. Support for the amendment is found in the specification at page 51, line 3, through page 52, line 3.

The OA notes that claims 45-60 are rejected upon the same grounds as claims 1-29, and are thus rejected for the same rationales. Applicants respond with the following comments:

Regarding claim 45, an independent claim, it has been amended in similar fashion to claim 30, noted above. Specifically, it has been amended to recite the ability of downloading applications from both trusted and untrusted sources, and upon downloading from an untrusted source, checking the program for aberrational code. Support for the amendment is found on page 27, line 3, through page 28, line 14, and FIG. 7. Applicants respectfully request reconsideration of the rejections to claims 45-60 per the comments regarding claims 1 and 30 above.

The OA notes that claims 61-73 are rejected upon the same grounds as claims 1-29, and are thus rejected for the same rationales. Applicants respond with the following comments:

Regarding claim 61, an independent claim, it has been amended in similar fashion to claim 30. Specifically, it has been amended to recite the ability of downloading applications from both trusted and untrusted sources, and upon downloading from an untrusted source, checking the program with an inspector. Support for the amendment is found on page 27, line 3, through page 28, line 14, and FIG. 7. As the arguments with respect to amended claim 30 are applicable to amended claim 61, they will not be recited again here. Applicants respectfully request reconsideration to the rejection of claims 61-73 per the comments directed to claims 1 and 30.

Note that claim 61, as amended, now recites a computer-based system comprised of various components (e.g. a deployment manager and an inspector). Such a physical structure is illustrated in FIG. 7, and is described in the corresponding specification.

U.S.S.N. 09/997,402

CONCLUSION

No amendment made was related to the statutory requirements of patentability unless expressly stated herein. No amendment made was for the purpose of narrowing the scope of any claim, unless Applicant has argued herein that such amendment was made to distinguish over a particular reference or combination of references.

For the above reasons, Applicants believe the specification and claims are now in proper form, and that the claims all define patentably over the prior art. Applicants believe this application is now in condition for allowance, for which they respectfully submit. If any matter may be more easily handled by telephone, the undersigned attorney welcomes telephone calls from the Examiner.

Respectfully submitted,



Philip H. Burrus, IV

Attorney for Applicants

Registration No.: 45,432

404-797-8111